

RoamAboutTM

ENJOY THE FREEDOM OF WIRELESS NETWORKING

R1 SOHO Access Point User's Guide

ENTERASYS.COM

ENTERASYS
NETWORKSTM

9033731-02



NOTE: Only qualified personnel should perform installation procedures.

NOTICE

Enterasys Networks and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS AND ITS LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS AND ITS LICENSORS HAVE BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© January 2002 by Enterasys NetworksTM, Inc.
All Rights Reserved. Printed in the United States of America.

Enterasys Networks
35 Industrial Way
Rochester, NH 03867

Part Number: 9033731-02

Enterasys, Enterasys Networks, RoamAbout and the RoamAbout logo are trademarks or registered trademarks of Enterasys Networks, Inc.

Apple, the Apple logo, Macintosh, and PowerBook are trademarks or registered trademarks of Apple Computer, Inc.

Microsoft, Windows, and Windows NT are either trademarks or registered trademarks of Microsoft Corporation.

PC Card is a trademark of PCMCIA.

All other trademarks and registered trademarks are the property of their respective holders.

Web Site: <http://www.enterasys.com/wireless>

FCC Notice

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



CAUTION: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada (Canada) - Class B Computing Device:

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Europe - EC Declaration of Conformity

This device complies with Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC.

VCCI Notice

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlußsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.

6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzan schlüßleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, das die Stromversorgung dieses Gerates nach der EN 60950 geprüft ist. Die Spg. Versorgungsteil-Ausgabewerte sollten +5V-Gleichstrom 2.A sein.

English Translation:

1. Please read these instructions carefully.
2. Keep this manual for future reference.
3. Before cleaning, unplug the power source. Do not use liquid or aerosol cleaners. For best results, use a moist cloth for cleaning.
4. The power jack should be close to the device and easily accessible.
5. Do not expose the device to humidity.
6. When setting up the device, make sure it is located on a solid, even surface. Tilting and falls may cause damage.
7. The ventilation openings are designed for air circulation, which protects the device from overheating. Make sure not to cover or block these openings.
8. When connecting to a power source, pay attention to the correct power values.
9. Do not put the power cable where people can fall over it. Do not put anything on the cable.
10. Pay attention to all notices and warnings on the device.
11. If you do not use the device for a longer while, unplug the power cord. This prevents damage in case of power surges.
12. Make sure no liquids or any items get into the device through the ventilation openings.
13. Never open the device. For reasons of electrical safety, the device must only be opened by authorized service personnel.
14. In the following situations, unplug the device from the power source and have it checked by a qualified service station:
 - a. Power cord or power plug is damaged.
 - b. Liquid has gotten into the device.
 - c. The device was exposed to humidity.
 - d. If the device does not function according to the operation manual, or you cannot improve its condition with the help of the manual.

e. The device has been dropped and/or the casing is damaged.
 f. If the device shows clear signs of a defect.

15. Make sure that the power source of this device complies with EN 60950. The power supply output values should be +5V DC 2.4A.

The sound pressure level at the workplace according to DIN 45 635 Part 1000 is 70dB(A) or less.

Restrictions for EU/EFTA Countries to R&TTE Directive:

AUS	B	DK	FIN	Member states in EU with restrictive use for this product are crossed out !
F	D	GR	IRE	<i>Les états membres de l'Union Européenne avec une utilisation restrictive de ce produit sont rayés !</i>
I	LUX	NL	P	<i>Mitgliedsstaaten der EU mit eingeschränkten Nutzungsrechten für dieses Produkt sind herausgestrichen</i>
E	S	UK		<i>Gli Stati membri nella Comunità Europea (EU) con restrizioni sull'uso di questi prodotti sono contrassegnati di seguito!</i>
CH				



Important Notice:

Low power radio LAN product operating in 2.4 GHz band for Home and Office environments.

Notice Importante:

Produit réseau local radio basse puissance opérant dans la bande de fréquence 2,4GHz pour les environnements bureautiques et résidentielles.

Wichtige Mitteilung

Low Power FunkLAN Produkt für den Home- und Office-Bereich, das im 2.4GHz Band arbeitet.

Nota Importante:

Apparati Radio LAN a bassa potenza, operanti a 2.4GHz, per ambienti domestico ed ufficio.

- Belgie B

Gebruik buiten gebouw alleen op kanalen 11 (2462 MHz), 12 (2467 MHz), en 13 (2472 MHz).

Voor privé-gebruik buiten gebouw over publieke grond over afstand kleiner dan 300m geen

registratie bij BIPT/IBPT nodig; voor gebruik over afstand groter dan 300m is wel registratie bij BIPT/IBPT nodig. Voor publiek gebruik buiten gebouwen is licentie van BIPT/IBPT verplicht. Voor registratie of licentie kunt u contact opnemen met BIPT.

- Belgium B	For outdoor usage only channel 11 (2462 MHz), 12 (2467 MHz), and 13 (2472 MHz) are allowed. For private usage outside buildings across public grounds over less than 300m no special registration with IBPT/BIPT is required. Registration to IBPT/BIPT is required for private usage outside buildings across public grounds over more than 300m. An IBPT/BIPT licence is required for public usage outside building. For registration and license please contact IBPT/BIPT.
- Belgique B	L'utilisation en extérieur est autorisé sur le canal 11 (2462 MHz), 12 (2467 MHz), et 13 (2472 MHz). Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.
- France F:	Bandé de fréquence restreinte : seuls les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) doivent être utilisés en France. Toute utilisation, qu'elle soit intérieure ou extérieure, est soumise à autorisation. Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour la procédure à suivre.
- France F:	Restricted frequency band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used in France. License required for every installation, indoor and outdoor installations. Please contact ART for procedure to follow.
- Deutschland D:	Anmeldung im Outdoor-Bereich notwendig, aber nicht genehmigungspflichtig. Bitte mit Händler die Vorgehensweise abstimmen.
- Germany D:	License required for outdoor installations. Check with reseller for procedure to follow
- Italia I:	E' necessaria la concessione ministeriale anche per l'uso interno. Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.
- Italy I:	License required for indoor use. Use with outdoor installations not allowed.
- the Netherlands NL	License required for outdoor installations. Check with reseller for procedure to follow.
- Nederlands NL	Licentie verplicht voor gebruik met buitenantennes. Neem contact op met verkoper voor juiste procedure

Europe – EU Declaration of Conformity

Hereby ENTERASYS NetworksTM declares that this RoamAbout IEEE 802.11 PC Card is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, Directive 89/336/EEC, and Directive 73/23/EEC.

ENTERASYS NetworksTM vakuuttaa täten että RoamAbout IEEE 802.11 PC Card tyypin laite on direktiivin 1999/5/EY, direktiivin 89/336/EEC ja direktiivin 73/23/EEC oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

ENTERASYS NetworksTM déclare que la carte PC RoamAbout IEEE 802.11 est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC, la directive 89/336/EEC, et à la directive 73/23/EEC.

Contents

Preface

Purpose of the Manual	ix
Intended Audience	ix
Organization of this Document	ix
Document Conventions	ix
Getting Help	x

1 Introduction

In This Chapter.	1-1
Overview	1-1
Features	1-2
Access and Application Support	1-3
LAN Connections	1-5
Wireless Connections.	1-6
Internet Connections	1-7
Printer Connections	1-7

2 Configuring the RoamAbout R1

In This Chapter.	2-1
Access Web Management	2-2
RI Management Navigation.	2-2
Setup Page Options.	2-2
Status Page	2-3
Networking and Client Services	2-4
Change Password	2-4
Set Time Zone.	2-4

Table of Contents

LAN Gateway and DHCP Settings.....	2-4
WAN Configuration	2-5
Dynamic IP Address – DHCP	2-5
Static IP Address – Fixed IP	2-5
PPP over Ethernet – PPPoE	2-5
Dial-up on Demand – Modem	2-6
DNS Configuration.....	2-6
Wireless Configuration	2-6
Channel and Network Name.....	2-6
Encryption.....	2-7
Configuring Client Services.....	2-7
Firewall Protection	2-7
Network Address Translation – NAT.....	2-8
Virtual Server	2-8
Enabling Special Applications	2-9
Virtual DMZ Host.....	2-9
Remote Management	2-9
Client Filtering	2-9
MAC Filtering.....	2-10
Viewing Network and Device Status.....	2-12
Using Tools	2-12

A Problem Solving

Preface

Purpose of the Manual

This manual provides configuration information for the RoamAbout R1 SOHO Access Point (hereafter called the RoamAbout R1). It also includes problem solving.

Intended Audience

This manual is intended for the customer who will set up the RoamAbout R1. This manual assumes that you already set up the clients and installed the RoamAbout R1. If not, please refer to the *RoamAbout R1 SOHO Access Point Setup and Installation Guide* for instructions.

Organization of this Document

This document is organized as follows:

Section	Description
Chapter 1	Provides an overview of the RoamAbout R1 and its features.
Chapter 2	Provides RoamAbout R1 configuration information.
Appendix A	Provides troubleshooting information.

Document Conventions

The following icons are used in this document:

Icon	Meaning
	CAUTION: Contains information essential to avoid personal injury, or damage to the equipment.
	NOTE: Calls the reader's attention to any item of information that may be of special importance.

Getting Help

For additional support related to this device or document, contact Enterasys Networks using one of the following methods:

World Wide Web: <http://www.enterasys.com/wireless>

Phone: North America: (603) 332-9400

Europe: 353 61 701 910

Asia: +800 8827-2878

Internet mail: support@enterasys.com

To send comments or suggestions concerning this document, contact the Enterasys Networks Technical Writing Department via the following e-mail

address: **TechWriting@enterasys.com**

Make sure you include the document Part Number in the e-mail message.

Before calling Enterasys Networks, please have the following information ready:

- Your Enterasys Networks service contract number
- A description of the problem
- A description of any action(s) already taken to resolve the problem
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (for example, layout and cable type)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, have you returned the device before, is this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Chapter 1

Introduction

This chapter provides an overview of the RoamAbout R1 and its features. Refer to the *RoamAbout R1 SOHO Access Point Setup and Installation Guide* for specification information.

In This Chapter

Information in this chapter is presented as follows:

Topic	Page
Overview	1-1
Features	1-2
Access and Application Support	1-3
LAN Connections	1-5
Wireless Connections	1-6
Internet Connections	1-7
Printer Connections	1-7

Overview

The RoamAbout R1 provides Internet access to multiple users by sharing a single-user account. The RoamAbout R1 serves as an access point, and includes a dual-port WAN (Wide Area Network) interface which allows you to connect to ADSL, xDSL, cable modem, or an ISDN TA or PSTN analog modem. The RoamAbout R1 provides extensive firewall protection and Virtual Private Network (VPN) services. It also provides print services for any client attached to a LAN (Local Area Network) port.

Features

You can connect the RoamAbout R1 to the Internet, or to a remote site, using its RJ-45 WAN port or RS-232 serial port. The RoamAbout R1 can also be connected directly to your PC, or to a LAN (local area network), using any of the three Fast Ethernet LAN ports or through the wireless interface. It can also function as a print server.

The RoamAbout R1 supports dial-on-demand for ISDN/PSTN service by automatically connecting to the Internet when there are requests, and terminating the connection if no further requests occur. This dual-port design also supports fail-over Internet access through the secondary WAN port (i.e., the serial port can be used for primary or backup Internet access).

Features

The RoamAbout R1 offers the following features:

- Internet connection to ADSL, xDSL, or Cable modem via a 10 Mbps WAN port
- Internet connection to ISDN TA or PSTN modem via an RS-232 console port
- Local network connection via 10/100 Mbps Ethernet ports or 11 Mbps wireless interface (supporting up to 32 mobile users)
- 802.11b Compliant – interoperable with multiple vendors
- Supports 40-bit and 128-bit WEP (Wired Equivalent Privacy)
- Built-in Print Server for any client attached to the LAN
- DHCP (Dynamic Host Configuration Protocol) for dynamic IP configuration, and DNS for domain name mapping
- Firewall with client privileges, hacker prevention, and NAT (Network Address Translation)

NAT also enables multi-user access with a single-user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, mail and Telnet)

- Virtual Private Network support using PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol) or IPSecurity pass-through
- User-definable application sensing tunnel supports applications requiring multiple connections
- Supports CHAP (Challenge Handshake Authentication Protocol) for dial-up identification
- Supports PPP (Point-to-Point Protocol) dial-in connection using the standard dial-up program
- Easy setup through a Java-enabled Web browser on operating systems that support TCP/IP

Access and Application Support

Many advanced applications are provided by the RoamAbout R1, such as:

- **Flexible LAN Access**

The RoamAbout R1 provides connectivity to 10/100 Mbps wired devices, as well as 11 Mbps wireless mobile users. The wireless interface makes it easy to create a network in difficult-to-wire environments, and to provide quick access to databases for wireless users.

- **Internet Access**

The RoamAbout R1 supports Internet access through an xDSL, Cable, ISDN or PSTN connection. Many DSL providers use PPPoE to establish communications with end users. The RoamAbout R1 includes a built-in client for PPPoE which eliminates the need to install this service on your computer.

- **Shared IP Address**

The RoamAbout R1 provides Internet access for up to 32 users with a shared IP address. Multiple users on your network can browse the Web at the same time using only one ISP account.

- **Virtual Server**

If you have a fixed IP address, you can set up the RoamAbout R1 to act as a virtual host for network address translation. Remote users can access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the RoamAbout R1 can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **User-Definable Application Sensing Tunnel**

You can define special applications that require multiple connections such as Internet gaming, videoconferencing, and Internet telephony. The RoamAbout R1 senses the application type and opens a multi-port tunnel for it.

- **DMZ Host Support**

DMZ (Demilitarized Zone) allows you to open up a client PC for two-way unrestricted Internet access. For example, you would use this feature if you have a client PC that cannot run an Internet application properly from behind the NAT firewall or after configuring the special applications feature. Using this feature creates a security risk and should only be used as a last resort.

- **Security**

The RoamAbout R1 supports security features that can deny Internet access to specified users, or filter all requests for specific services. The RoamAbout R1's firewall can also block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Virtual Private Network**

The RoamAbout R1 supports three of the most commonly used VPN protocols – PPTP, L2TP and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then any of these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network). The VPN protocols supported by the RoamAbout R1 are briefly described below.

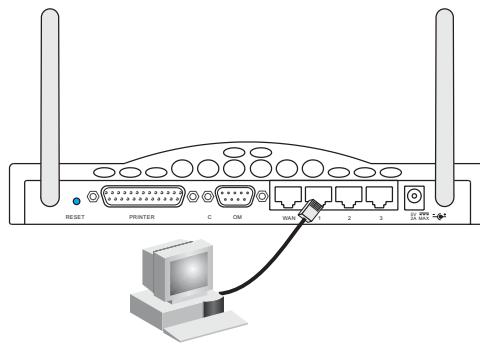
- Point-to-Point Tunneling Protocol – Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
- Layer Two Tunneling Protocol – Includes most of the features provided by PPTP, but has less overhead and is more suited for managed networks.
- IP Security – Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

LAN Connections

The three LAN ports on the RoamAbout R1 can auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half-duplex or full-duplex. These LAN ports also support auto-configuration for pin signals (auto-MDI/MDI-X) that allows you to use straight-through cable for connecting the RoamAbout R1 to any network device. Refer to the *RoamAbout R1 SOHO Setup and Installation Guide*.

Use twisted-pair cable to connect any of the three LAN ports on the RoamAbout R1 to an Ethernet adapter on your PC. Otherwise, you can cascade any of LAN ports on the RoamAbout R1 to an Ethernet hub or switch, and then connect your PC (or other network equipment) to the hub or switch.

Figure 1-1: LAN Connection



Wireless Connections

Install a PC Card in each computer that will be connected to the Internet or your local network via radio signals.

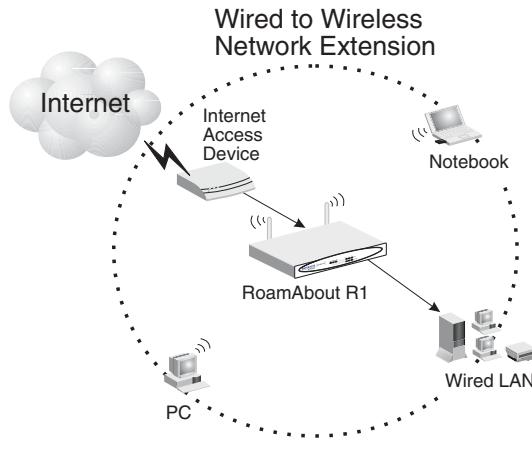
Rotate both antennas on the back of the RoamAbout R1 to the desired position. For more effective coverage, position one antenna along the vertical axis and the other along the horizontal axis. Place the RoamAbout R1 in a position that is located in the center of your wireless network. Normally, the higher you place the antenna, the better the performance.

Computers equipped with PC Cards can communicate with each other as an independent wireless LAN by configuring each computer to the same radio channel. However, the RoamAbout R1 can provide access to your wired/wireless LAN, or to the Internet, for all wireless workstations. Each wireless PC in this network infrastructure can talk to any computer in the wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure or over the Internet via the RoamAbout R1.

The wireless infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also doubles the effective wireless transmission range for wireless PCs by retransmitting incoming radio signals through the RoamAbout R1.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in **Figure 1-2**.

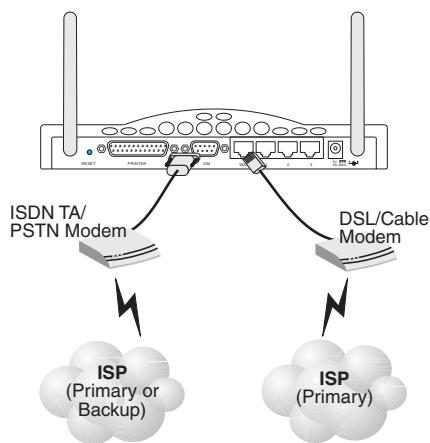
Figure 1-2: WLAN Configuration Example



Internet Connections

If Internet services are provided through an xDSL or cable modem, use unshielded or shielded twisted-pair Ethernet cable (Category 3 or greater) with RJ-45 plugs to connect the broadband modem directly to the WAN port on the RoamAbout R1. Use either straight-through or crossover cable depending on the port type provided by the modem. For ISDN or PSTN service, attach the access device to the RS-232 serial port on the RoamAbout R1. Refer to the *RoamAbout R1 SOHO Access Point Setup and Installation Guide*

Figure 1-3: WAN Connection Example



Printer Connections

If you connect a printer to the RoamAbout R1, all the computer users connected to your LAN can have access to the printer. Connect a standard parallel printer cable to the Printer port on the RoamAbout R1, and configure the printer server as described in the *RoamAbout R1 SOHO Access Point Setup and Installation Guide*.

Chapter 2

Configuring the RoamAbout R1

A Web browser is used to configure the RoamAbout R1, view statistics, and to monitor network activity. The RoamAbout R1 can be configured by any Java-supported browser, including Internet Explorer Version 5.0 (or higher) and Netscape Navigator Version 4.0 (or higher).



This manual assumes that you already set up the clients and installed the RoamAbout R1. If not, please refer to the RoamAbout R1 SOHO Access Point Setup and Installation Guide for instructions.

In This Chapter

Information in this chapter is presented as follows:

Topic	Page
Access Web Management	2-2
RI Management Navigation	2-2
Networking and Client Services	2-4
Wireless Configuration	2-6
Configuring Client Services	2-7
Viewing Network and Device Status	2-12
Using Tools	2-12

Access Web Management

To access the RoamAbout R1's management interface, enter the IP address of the RoamAbout R1 in your Web browser (<http://192.168.2.1>). The Login screen prompts you for a password. The default password is *password*.

The Main page links are used to navigate to other pages that display configuration parameters and statistics. You can define system parameters, manage and control the RoamAbout R1 and its ports, or monitor network conditions.

RI Management Navigation

The RoamAbout R1's management interface includes four key pages – Setup, Status, Tools and Help. The Status and Help pages provide general information on the current settings and how to configure the RoamAbout R1. The Setup page is used to configure the LAN, WAN and wireless interface, as well as other advanced functions. While the Tools page is used to reset the RoamAbout R1, restore the factory settings, or upgrade firmware.

Once a configuration change has been made on a page, be sure to click on the **Save** button located at the bottom of the page to save the new configuration change.



*To ensure a proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the page **Tools** / **Internet Options** / **General** / **Temporary Internet Files** / **Settings**, the setting for **Check for newer versions of stored pages** should be **Every visit to the page**.*

Setup Page Options

The Setup page allows you to configure TCP/IP settings and client services. **Table 2-1** provides brief descriptions of the options.

Table 2-1: Setup Page

Setup Page	Description
Change Password	Sets the password for administrator access.
Set Time Zone	Sets the local time zone.
LAN	Sets the TCP/IP configuration for the RoamAbout R1 LAN interface and all DHCP clients.
WAN	Specifies the Internet connection type: DHCP host configuration, fixed IP and gateway address, PPPoE configuration, or dial-up modem.

Setup Page	Description
DNS	Specifies DNS servers to use for domain name resolution.
Wireless	Configures the radio frequency, domain, and encryption for wireless communications.
Advanced Settings	<p>Configures a variety of packet filtering and specialized functions, including:</p> <ul style="list-style-type: none"> • Firewall • NAT • Virtual Server • Special Application • Virtual DMZ Host • Remote Management • Client Filtering • MAC Filtering

Status Page

The Status page allow you to display connection status, key interface settings, and the firmware and hardware version numbers. **Table 2-2** provides brief descriptions of the options.

Table 2-2: Status Page

Status Page	Description
INTERNET	Displays WAN connection type and status.
ROAMABOUT R1	Displays system IP settings, the status for DHCP, NAT and Firewall services, as well as the wireless interface settings.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, as well as the hardware version and serial number.
Security Log	Displays any illegal attempts to access your network.
DHCP Client Log	Displays information on all DHCP clients attached to your network.

Networking and Client Services

Use the Setup page to configure the LAN interface (including TCP/IP parameters for the RoamAbout R1's gateway address, DHCP address pool for dynamic client address allocation), the WAN connection options, DNS domain name mapping, the wireless interface, and other advanced services.

You can use the Setup Wizard by clicking on the **Start** button at the bottom of the first page.

Change Password

Use this page to restrict management access based on a specific password. You need a password to access the configuration options provided by the Setup and Tools pages. By default, the password is *password*. It is strongly recommended that you change the default password as soon as possible. The Status and Help pages are not password protected.

Passwords can contain from 3 to 12 alphanumeric characters, and are not case sensitive.



NOTE *If your password is lost, or you cannot gain access to the management interface, press the **Reset** button on the back panel for at least 5 seconds to restore the factory defaults.*

Set Time Zone

Set the time zone for the RoamAbout R1. This information is used for log entries and client filtering.

LAN Gateway and DHCP Settings

Configure the gateway address of the RoamAbout R1. To dynamically assign the IP address for client PCs, enable the DHCP Server, set the lease time, and then specify the address range. Also remember to configure all of your client PCs for dynamic address allocation.

Valid IP addresses consist of four numbers, and are separated by periods. The first three fields are the network portion, and can be from 0–255, while the last field is the host portion and can be from 1–254. Do not include the gateway address of the RoamAbout R1 in the client address pool.

WAN Configuration

Specify the WAN connection type required by your Internet Service Provider, then click on **More Configuration** to provide detailed configuration parameters for the selected connection type.

Specify one of the first three options to configure a WAN connection through the RJ-45 port (i.e., a connection to an xDSL modem or Cable modem). Specify the **Dial-up on Demand** option to configure a WAN connection through the serial port (i.e., a connection to an ISDN TA or PSTN modem).



If WAN connections are configured for both the RJ-45 and serial port, the serial port will be used as a backup Internet connection if the primary RJ-45 WAN connection fails.

Dynamic IP Address – DHCP

The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the RoamAbout R1. Use this address when registering for Internet service, and do not change it unless required by your ISP. You can determine the RoamAbout R1's MAC address by clicking on **Status** in the Main page. You can use the **Clone MAC Address** button to copy the MAC address of the Ethernet Card installed by your ISP (in your PC) and replace the WAN MAC address with this MAC address.

Static IP Address – Fixed IP

If your Internet Service Provider assigned a fixed address, enter the assigned address and subnet mask for the RoamAbout R1, then enter the gateway address of your ISP.



You may need a fixed address if you want to provide Internet services, such as a Web server or FTP server.

PPP over Ethernet – PPPoE

Enter the PPPoE user name and password assigned by your ISP. The Service Name is normally optional, but may be required by some providers.

Dial-up on Demand – Modem

If you are accessing the Internet via an ISDN TA or PSTN modem attached to the serial port on the RoamAbout R1, then you must specify your account information as described below.

- *Check if you only use a dial-up modem to connect to the Internet.* – If the serial port is used for primary Internet access, select this item. If not selected, then this connection will only be used for backup access if the primary WAN link fails.
- *Dial-Up Service Phone Number* – Enter the phone number your service provider has given to you for Internet access.
- *Dial-Up Account Information* – Enter your ISP account user name and password.
- *Assigned ISP IP address* – If you are assigned a dynamic IP address every time you dial up, select **No** for this item. However, if your ISP has assigned a fixed IP address for you to use, select **Yes** for this item and enter the IP address and subnet mask.



If your ISP has given you a secondary phone number, or if you have a secondary Internet service account, then fill in the relevant fields under Secondary Dial-up.

DNS Configuration

Domain Name Servers are used to map an IP address to the equivalent domain name (e.g., www.enterasys.com). Your ISP should provide the IP address for one or more domain name servers. Enter those addresses on the page.

Wireless Configuration

To configure the RoamAbout R1 as a wireless access point for wireless clients (either stationary or roaming), you need to define the radio channel, the domain identifier, and encryption options.

To set up the wireless channel and the network name, click on **Wireless** and then the **START** button at the bottom of the first page, or you can select **Channel and Network Name** and **Encryption** from the Setup page.

Channel and Network Name

You must specify a common radio channel and Wireless Network Name (or SSID) to be used by the RoamAbout R1 and all of your wireless clients. Be sure you configure all of your clients to the same values.

Encryption

If you are transmitting sensitive data across wireless channels, you should enable encryption. Encryption requires you to use the same set of encryption keys for the RoamAbout R1 and all of your wireless clients. The RoamAbout supports 40-bit or 128-bit WEP (Wired Equivalent Privacy) encryption.

- The position of each key is important. The clients must enter the same key in the same position to communicate with the RoamAbout R1.
- 40-bit encryption uses 5-pair ASCII key (or 10 hexadecimal digits).
- 128-bit encryption uses 13-pair ASCII key (or 26 hexadecimal digits) and supports both 40-bit and 128-bit encryption.
- ASCII keys are case-sensitive.
- Valid Hexadecimal digits are 0-9 or A-F.



Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Configuring Client Services

The RoamAbout R1 includes a broad range of client services, including firewall protection, network address translation, virtual server, connection support for special applications, and restricted Internet access for specified clients. You can configure these functions using the Setup Wizard by clicking on **Start**, or by selecting specific items from the page.

Firewall Protection

The RoamAbout R1's firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network users.

Network Address Translation – NAT

Network Address Translation can be used to give multiple users access to the Internet with a single user account, or to map the local address for an IP server (such as Web or FTP) to a public address. This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.



NAT must be enabled to provide multi-user access to the Internet, or to use the Virtual Server function.

Virtual Server

If you configure the RoamAbout R1 as a virtual server, remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. Depending on the requested service (TCP/UDP port number), the RoamAbout R1 redirects the external service request to the appropriate server (located at another internal IP address).

The WAN interface must have a fixed IP address to utilize this function. For example, if you set Type/Public Port to TCP/80 (HTTP or Web) and the Private IP/Port to 192.168.2.2/80, then all HTTP request from outside users will be transferred to 192.168.2.2. Therefore, by just entering the IP Address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

Some of the more common TCP service ports include:

- HTTP: 80
- FTP: 21
- Telnet: 23
- POP3: 110.

Enabling Special Applications

Some applications require multiple connections, such as Internet gaming, videoconferencing, Internet telephony and others. These applications may not work when Network Address Translation (NAT) is enabled.

Specify the port normally associated with an application in the **Trigger Port** field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.



If an application still cannot function correctly after enabling multiple ports, you may have to open the client PC for full Internet access using the DMZ Host option.

Virtual DMZ Host

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, or after configuring the Special Applications function, you can open the client up to unrestricted two-way Internet access.



Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks. Only use this option as a last resort.

Remote Management

By default, management access is only available to users on your local network. You can manage the RoamAbout R1 from a remote host by adding the IP address of an administrator in the Remote Management page.



- *If you specify an IP address of 0.0.0.0, any host in your local network can manage the RoamAbout R1.*
- *Only one management session can be logged in at a time. You must log out of the current session on the system before you can manage the RoamAbout R1 from a different system.*

Client Filtering

You can filter Internet access for local clients based on IP address, application type (i.e., HTTP port), and time of day.

MAC Filtering

You can filter Internet access for local wired and wireless clients based on the MAC address.

MAC Address Control

Every client that connects to the network has a unique MAC (Media Access Control) address on his or her Ethernet adapter. An administrator can have more control- and more security- over the network by specifying which MAC addresses are allowed to access the RoamAbout R1. You can enable this feature by selecting **Enabled**.

Connection Control

Connection control allows an administrator to allow or deny clients access to the RoamAbout R1 and the Internet. Select **Connection control** to control which of the wired and wireless clients will be able to connect to the RoamAbout R1 and to the Internet. If a client is denied connection to this device, it means that the client can't access the Internet and some network resources. Select to **Allow** or **Deny** clients whose MAC addresses are not listed in the **Control table**.

- When a wired client is allowed to connect to the RoamAbout R1 it has full access to the Internet and network resources.
- When a wired client is not allowed to connect to the RoamAbout R1 it can communicate with the other clients on the wired LAN, but cannot:
 - Connect to the Internet
 - Use the Print Server function
 - Communicate with the clients on the wireless LAN
 - Use the RoamAbout R1's Web configuration

Association Control

The Association process is the exchange of information between wireless clients and a wireless access point to establish a link between them. A wireless client is capable of transmitting and receiving data to an access point only after the association process is successfully completed.

Association control allows an administrator to allow or deny wireless clients from linking to the RoamAbout R1. Select **Association control** to control which of the wireless clients will be able to associate with the wireless LAN. If a client is denied association to the wireless LAN, it means that the client can't send or receive any data through the RoamAbout R1. Choose **Allow** or **Deny** to allow or deny clients whose MAC addresses are not listed in the **Control table**.

When a wireless client is allowed to associate with the wireless LAN and connect to the RoamAbout R1, it has full access to the Internet and network resources.

When a wireless client is not allowed to associate with the wireless LAN, it cannot:

- Communicate with any other clients on the LAN (neither wired nor wireless)
- Connect to the Internet
- Use the Print Server function
- Use the RoamAbout R1's Web configuration
- Connect to the RoamAbout R1

When a wireless client is allowed to associate with the wireless LAN, but not connect to the RoamAbout R1, it can communicate with other clients on the wireless LAN, but cannot:

- Communicate with any clients on the wired LAN
- Connect to the Internet
- Use the Print Server function
- Use the RoamAbout R1's Web configuration

Association control has no affect on wired clients.

Viewing Network and Device Status

The Status page displays the connection status for the WAN, WLAN, and LAN interfaces. It also displays the firmware and hardware version numbers, illegal attempts to access your network, as well as all DHCP clients connected to your network.

The following information is displayed on the page:

Field	Description
INTERNET	Displays connection type and status
ROAMABOUT R1	Displays system IP settings, the status for DHCP, NAT and Firewall services, as well as the wireless interface settings.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, as well as the hardware version and serial number.
Security Log	Displays any illegal attempts to access your network.
DHCP Client Log	Displays information on all DHCP clients on your network.

Using Tools

Use the Tools page to reboot, restore to factory defaults, and upgrade the firmware.

Field	Description
Reset RoamAbout R1	Reboots the RoamAbout R1 and retains the current SAVED configuration settings.
Restore Factory Defaults	Removes all configuration settings and restores the RoamAbout R1 back to its original factory state.
Update Firmware	Allows you to check the Enterasys Networks Wireless Web site for upgrades and upgrade the RoamAbout R1 with the new firmware.

You can also reset the RoamAbout R1 back to its original factory by pressing the Reset button on the back panel for 5 seconds.

Appendix A

Problem Solving

This Appendix describes common problems you may encounter and possible solutions. The RoamAbout R1 can be easily monitored through its panel indicators to identify problems.

Troubleshooting Chart	
Symptom	Action
Power LED is Off	<p>The External power supply has failed or is disconnected.</p> <ul style="list-style-type: none">Check connections between the RoamAbout R1, the external power supply, and the wall outlet.If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. <p>If the unit powers off after running for a while, check for loose power connections, power losses or surges at the power outlet.</p> <p>If you still cannot isolate the problem, the external power supply may be defective. In this case, contact Enterasys Networks Technical Support for assistance.</p>
Link LED is Off	<ul style="list-style-type: none">Verify that the RoamAbout R1 and attached device are powered on.Verify that the cable is plugged into the RoamAbout R1 and the corresponding device.Verify that the proper cable type is used and its length does not exceed specified limits.Verify that the network interface on the attached device is configured for the proper communication speed and duplex mode.Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

Troubleshooting Chart	
Symptom	Action
Network Connection Problems	
Cannot Ping the RoamAbout R1 from the attached LAN, or the RoamAbout R1 cannot Ping any device on the attached LAN	<ul style="list-style-type: none"> Verify that IP addresses are properly configured. For most applications, you should use the RoamAbout R1's DHCP function to dynamically assign IP addresses to any host on the attached LAN. If you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the RoamAbout R1 and the attached LAN devices. Verify that the device you want to ping (or from which you are pinging) has been configured for TCP/IP.
Wireless users cannot access the RoamAbout R1	<ul style="list-style-type: none"> Verify that the RoamAbout R1 and all wireless users are configured to use the same radio channel, wireless domain (Wireless Network Name, SSID), and encryption keys. Verify that all wireless users are within range of the RoamAbout R1. <ul style="list-style-type: none"> - Indoors: Up to 160 ft. (50 m) - Outdoors: up to 480 ft. (50 m)
Management Problems	
Cannot connect using the Web browser	<ul style="list-style-type: none"> Verify that the RoamAbout R1 was configured with a valid IP address, subnet mask and default gateway. Verify that you have a valid network connection to the RoamAbout R1, and that the port you are using has not been disabled. Check the network cabling between the management station and the RoamAbout R1. Verify that you logged out of the management station that you were previously using to manage the RoamAbout R1. If that session timed-out, you must log back into that management station and log out before you can manage the RoamAbout R1 from any other management station
Forgot or lost the password	Press the RESET button on the rear panel for 5 seconds to restore the factory defaults. The default password is <i>password</i> .
Printer Server	
The printer cannot print or prints illegible text.	Verify that the parallel cable between the RoamAbout R1 and printer is connected, and in good condition